UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/641,156	08/17/2000	David M. Chess	YOR9-1999-0564	4738

7590 08/08/2005

Harry F Smith Esq
Ohlandt Greeley Ruggiero & Perle LLP
Suite 903
One Landmark Square
Stamford, CT 06901

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/641,156	CHESS ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication filed on: 9 May 2005 with an original application filed 17 August 2000.

2. Claims 1-52 are currently pending in this application. Claims 1, 26, 51, and 52 are independent claims. Claims 1, 3-18, 21-24, 26, 28-44, 46-49, and 51 have been amended. Claim 52 is new.

Claim Objections

3. Claim 46 is objected to because of the following informalities: on line two the word "appliance" is misspelled. Appropriate correction is required.

Response to Arguments

4. Applicant's arguments filed on 13 May 2005 have been fully considered but they are moot due to new grounds of rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1, 8, 13, 14, 26, 32, 37, 38, and 51** are rejected under 35 U.S.C. 102(e) as being anticipated by Bouthillier et al. U.S. Patent No. 6,021,497 (hereinafter '497).

As to independent claim 26, "A method for the secure installation and use of an information system comprising a plurality of nodes, where said plurality of nodes include at least one information appliance" is taught in '497 col. 2, lines 15-30 (note "information appliance" is interpreted as having the same meaning as "computers")

and at least one security console, said method comprising steps of" is shown in '497 col. 3, lines 3-8;

"providing at least one data-carrying object containing security-related data; and inserting the data-carrying object into a selected one of a plurality of object receptacles that comprises a portion of at least one of the nodes, wherein the selected object receptacle is one of two or more of said receptacles that are connected to said security console" is disclosed in '635 col. 1, lines 55-67;

"the data-carrying object being inserted into the receptacle that reads out the security-related data wherein a desired security configuration of said information system is based on the security-related data and the selected object receptacle" is taught in '497 col. 2, lines 3-14.

As to dependent claim 32, "wherein the data carrying object comprises a first one of first and second data-carrying objects that are provided as a pair, wherein the selected receptacle comprises a first receptacle wherein the information appliance is intended to be used for indicating, from security-related data contained on said first carrying objects, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second one of the receptacles has an output coupled to the information appliance for indicating, from security- related data contained

on said second, that the security console is authorized to fulfil and originate requests for information appliance resources, including information" is shown in '497 col. 5, lines 10-30.

As to dependent claim 37, "wherein data-carrying objects is one of a group of at least three data-carrying objects, and where access to a resource of the information appliance, including information, is obtained by providing one subset of data-carrying objects from said group to a receptacle associated with a requestor of the resource, and a disjoint set of data-carrying objects from said group is provided to the receptacles connected to the security console" is disclosed in '497 col. 5, lines 10-30.

As to dependent claim 38, "wherein identifications of all individual data-carrying objects in the group can be ascertained by viewing the Security console, even if some subset of the data-carrying objects are provided to a receptacle associated with a requestor of the resource" is taught in '497 col. 3, lines 3-8.

As to independent claim 1, this claims is directed to the apparatus of the method of claim 26 and is similarly rejected along the same rationale.

As to independent claims 51, this claims is directed to computer-readable storage medium of the method of claim 26 and is similarly rejected along the same rationale

As to dependent claims 8, 13, and 14, these claims incorporate substantially similar subject matter as in cited in the claims 32, 37, and 38 above and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 2, 4, 5, 10, 11, 15, 16, 18-22, 27, 29, 34, 35, 39, 40, and 42-47,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '497 in further view of Reardon U.S. Patent No. 6,212,635 (hereinafter '635).

As to dependent claim 27, the following is not taught in '497 **"wherein the data-carrying object stores the security-related data in a form that can be read-out by one of an electrical sensor, an optical sensor, or a magnetic sensor"** however '635 teaches "Token: A removable memory device capable of storing one or more encryption keys. This token may be as simple as a magnetic strip or as complex as a PCMCIA card. Token Reader: An input device by which means the security gateway can read the information encoded on a token" in col. 7, lines 13-20.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network security system taught in '497 to include a means enhance software protection. One of ordinary skill in the art would have been motivated to perform such a modification because of the specialized computer hardware available see '635 (col. 1, lines 47 et seq.) "Software protection of computer data can be enhanced by the use of specialized computer hardware that provides additional security functions ... enhancing security by making some security functions independent of the CPU. In Reardon's invention, these hardware secured parameters require a user to insert and activate a CPU independent hardware switch to change or alter the security parameters".

As to dependent claim 29, "wherein said information appliance has associated therewith the security-related data of said data-carrying object the information appliance is intended to be used for indicating that the information appliance is one of a trusted information appliance" is disclosed in '497 col. 5, lines 10-31 "Referring now to FIGS. 1, 3a, 3b, and 5, there is shown a data relay switch control circuit 101 which includes three card readers 120, 122 and 124 associated with respectively first, second and third data channels 87, 89 and 91 of the secured network system 10 of FIGS. 3a and 3b. Terminals 112, 114, 116 and 118 are terminals on readykey controller 12. Terminal 118 connects card reader 120 to readykey controller 12, terminal 116 connects card reader 122 to readykey controller 12 and terminal 114 connects card reader 124. Each terminal 114, 116 and 118 and its associated card reader 124, 122 and 120 includes a data line SIG which is used to transfer data between readykey controller 12 and card readers 124, 122 and 120. The data relay switch control circuit 101 has a control relay contact RC4 which is controlled by readykey controller 12. When readykey controller 12 closes control relay contact RC4, channel 87, 89 or 91 on data relay switch 26 (FIGS. 3a and 3b) can be enabled respectively by control relay contacts RC1, RC2 or RC3. Control relay contacts RC1, RC2 or RC3 are also controlled by readykey controller 12";

"or an untrusted information appliance" is taught in '635 col. 7, lines 34-36 "key pair used by a certifying authority to assist in anonymous but traceable transactions wherein the anonymous user's identity and Digital Certificate is sealed with AK.1B. AK.1R is divided and placed in escrow so the anonymous users Digital Certificate and identity can be recovered, with proper authorization such as a court order, in the event there is a subsequent criminal investigation or civil dispute".

As to dependent claim 34, "wherein the data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are the same shape, and no two data-carrying objects not in the same pair are the same shape" is taught in '635 col. 25, lines 34-37 "Other mechanical or chemical marking techniques migh also be employed to create special diskettes that can be used as tokens wherein each token would have a unique "finerger-print." The diskette media might be precisely or randomly scarred with lasars, chemical spattering, ion bombardment, or other means".

As to dependent claim 35, "wherein the data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are imprinted with a same visible identification information, and no two data-carrying objects not in the same pair are imprinted with the same visible identification information" is shown in '635 col. 25, lines 34-37.

As to dependent claim 39, "wherein a utilization of different disjoint subsets of the data-carrying objects in said group indicates different levels of trust to be granted to the requestor with respect to the resource" is shown in '635 col. 12, lines 1-9 "Tokens can be created for each individual and also for specific applications. For example, a corporate accountant might have two tokens. The first would be a general use token that provides him with access to all the general purpose programs he might need such as word processing and Internet access with the exception of access to the accounting books. The second token that gives him access to the accounting books might be separately stored under lock and key, thus providing an additional level of security".

As to dependent claim 40, "wherein a utilization of different disjoint subsets of the data-carrying objects in said group indicates different levels of authorization to be granted to the requestor with respect to the resource" is disclosed in '635 col. 12, lines 1-9.

As to dependent claim 42, "in which access to the resource is denied unless every data-carrying object of the group is inserted into a receptacle" is taught in '635 col. 19, lines 36-39 "it would be possible and advisable to divide the SYSTEM MASTER KEY into several parts that would be placed in escrow with two or more trusted corporate officials. These escrowed keys would be useless until they are used in combination with each other so that the security gateway implementing the system wide changes can reconstruct the actual SYSTEM MASTER KEY".

As to dependent claim 43, "wherein said information appliance is one of a group of information appliances, and further comprising a step of adding a newly-obtained information appliance to a group of authorized information appliances, on behalf of a principal, by inserting a data-carrying object representing the principal to a receptacle of the information appliance" is shown in 635 col. 14, lines 21-42 "The following describes one of many ways in which the security gateway could be used to install or upgrade the SHELL ... While the system is powered down, the MASTER TOKEN would be loaded into the token reader".

As to dependent claim 44, " wherein the data-carrying object representing the principal contains data which includes at least one secret known only to the principal" is disclosed in '635 col. 10, lines 64-65 "A PIN would be selected and encrypted and stored on the MASTER TOKEN with additional security parameters, passwords".

As to dependent claim 45, "wherein the secret known only to the principal comprises the private half of a public-private key pair associated with an asymmetric cryptosystem" is taught in '635 col. 11, lines 1-9 "as the private key of the MASTER TOKEN holder and can be used for verification of identity".

As to dependent claim 46, "wherein said information appliance is authorized on behalf of a certain principal, wherein said certain principal, and said information appliance authorized to act on behalf of the principal, is granted a certain level of access to a certain resource by inserting, to a receptacle associated with an information appliance representing the resource, a data-carrying object representing the principal" is shown in '635 col. 11, lines 10-14 "After this first initialization, the MASTER TOKEN can be used to reconfigure security parameters or to create new tokens for one or more users with rights either equivalent to those associated with the MASTER TOKEN, or more commonly, with restricted rights. Every time the security gateway creates a new token, it would create a unique key pair U.X for the person to whom the token is issued, User X. U.XR and an associated PIN would be stored on the token in a form encrypted with SG.1B. U.XB would be stored in the security controllers restricted memory or, if desired, "published" in a file accessible to the CPU or computer network".

As to dependent claim 47, "wherein data contained in the additional data-carrying object representing the principal comprises the public half of a public-private key pair associated with an asymmetric cryptosystem" is disclosed in '635 col. 11, lines 1-9.

As to dependent claim 4, "wherein said data-carrying object is temporarily made readable by said selected receptacle in order to initiate said security configuration" is taught in '635 col. 12, lines 20-28 "Most ideally, the security gateway would automatically sense when a token is inserted into the token reader and the security SHELL would automatically activate a window requesting the user to enter his or her PIN. Alternatively, the user can activate a program that instructs the computer to log on a new user. After confirmation of the PIN, the user could be instructed to remove the token before allowing access to ensure that user does not forget to remove the token and properly secure it".

As to dependent claims 2, 5, 10, 11, 15, 16, and 18-22, these claims incorporate substantially similar subject matter as in cited in the claims 27, 29, 34, 35, 39, 40, and 43-47 above and are rejected along the same rationale.

9. **Claim 52** is rejected under 35 U.S.C. 103(a) as being unpatentable over '497 in further view of Fisher, Jr. et al. U.S. Patent No. 6,718,319 (hereinafter '319).

As to independent claim 52, "Apparatus for the secure installation and use of an information system comprising: a plurality of nodes, where said plurality of nodes includes at least one information appliance" is taught in '497 col. 2,

lines 15-30;

"and at least one security consol" is shown in '497 col. 3, lines 3-8;

"at least first and second physical data-carrying objects each containing security–related data; and a first object receptacle and a second object receptacle that are connected to said security console, a third object receptacle connected to said information appliance,

said first physical data-carrying object being inserted into a selected one of said first and second object receptacles that reads out the associated security–related data, said second physical data-carrying object being inserted into said third object receptacle that reads out associated security-related data" is shown in '497 col. 3, lines 3-8;

the following is not taught in '497 **"wherein a desired security configuration of said information system is based on said security–related data and said selected on of said first and second object receptacles and wherein said security configuration gives access to a resource of one of said information system by said information appliance and said information appliance by said security console"** however '319 teaches "These and other objects of the present application are further fulfilled by providing a method for communicating with a card … These and other objects of the present application are still yet further fulfilled by providing an apparatus for formatting a card reader, comprising: a first memory for prestoring a plurality of card reader configuration files for configuring a software tool for formatting the card reader; a selection function for selecting one of the prestored card reader configuration files based upon card reader type; a dynamic memory for storing the card reader configuration file selected based upon card reader type, wherein the software tool is configured based upon the stored card configuration file, the selection function further selects at least one command for formatting the card reader, and the selected at least one command is stored in memory of the card reader; and a processing function for formatting the card reader based upon the at least one selected and stored command" in col. 2, lines 35-64.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network security system taught in '497 to configure the various smartcards and

smartcard readers. One of ordinary skill in the art would have been motivated to perform such a modification because utilizing different smart cards and smart card readers can be difficult see '319 (col. 1, lines 57 et seq.) "In a system utilizing different smart cards and smart card readers, such a system was quite cumbersome, mostly because of the specialized smart card software that was provided by the hardware manufactures. Many of the tools for creating specialized smart cards to comply with a user's desired specifications were not high-level tools and were not easy to use. The tools did not create any common way to work with different smart cards and readers, and there was no existing development tool that permitted development of an application for different readers and cards".

10. **Claims 3, 6, 7, 28, 30, and 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over '497, in further view of '635 in further view of Reardon U.S. Patent No. 5,434,562 (hereinafter '562).

As to dependent claim 28, "wherein the data-carrying object either" and **"or is temporarily inserted in or otherwise made readable by the selected receptacle either before or during the operation of the information system"** is taught in '635 col. 12, lines 25-28 "the user could be instructed to remove the token before allowing access";

the following is not taught in the combination of '497 and '635 "**remains inserted in the selected receptacle during the operation of the information system"** however '562 teaches "Typically, the disabling of the peripheral device is executed by the user operating a switch, which may be of a keylocking type, which fully or partially disables the peripheral device as long as the switch is activated" in col. 3, lines 41-44.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network security system taught in '497 and '635 to include a means to protect devices as long as a key is active. One of ordinary skill in the art would have been motivated to perform such a modification to protect a computer system from unauthorized access see '562 (col. 1, lines 45 et seq.) "By providing complete user control over a computer's access to its peripheral devices, this invention allow the user to implement greater security precautions against unauthorized programs or users".

As to dependent claim 30, "wherein said information appliance is given access to information system resources, including information, by inserting an additional data-carrying object associated with the security console into at least one of the receptacles" is taught in '635 col. 11, lines 33-53 "In a typical application, the User X would place the token, 16, in token reader, 14. The token reader would transfer information from the token to the security gateway ... While such peripherals cannot be protected in the same fashion as "down line" peripherals which have the security gateway interposed between themselves and the CPU, the security gateway can still provide some protection for the "up line" peripherals";

"that has an output that is coupled to the information appliance" is shown in '562 col. 3, lines 50-52 "physically disconnect thye power supply to the mass storage media device and/or the communication link to the network".

As to dependent claim 31, "wherein each of the information appliance and the security console have associated therewith first and second corresponding data-carrying

object" is disclosed in '635 col. 12, lines 1-2 "Tokens can be created for each individual and also for specific applications"

"respectively, wherein said selected receptacle comprises a first receptacle wherein the information appliance is intended to be used for indicating, from security-related data contained on the first data-carrying object associated with the information appliance, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second one of the receptacles has an output coupled to the information appliance for indicating, from security-related second data contained on the data-carrying object associated with the security console, that the security console is authorized to fulfil and originate requests for information appliance resources, including information" is taught in '542 col. 3, lines 29-39 "This invention describes a means and process by which to disable the computer's access to all or part of a computer's memory system or associated peripherals".

As to dependent claims 3, 6, and 7, these claims incorporate substantially similar subject matter as in cited in the claims 28, 30, and 31 above and are rejected along the same rationale.

11. **Claims 9, 23, 24, 25, 33, 48, 49, and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over '497 in further view of '635 in further view of Flyntz U.S. Patent No. 6,389,542 (hereinafter '542).

As to dependent claim 33, the following is not taught in the combination of '497 and '635 **"wherein said selected receptacle comprises a first receptacle, and wherein an insertion of the data-carrying object into said first receptacle indicates different security-related information than inserting the data-carrying object into a second one of said twor or more receptacles"** however '542 teaches "if the removable memory for the second security subsystem is correctly inserted in the memory receptacle. In response to the first activation signal, the first electronically activated switch disconnects the common contact from the first contact and connects the common contact with the second contact" in col. 3, lines 30-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network security system taught in '497 and '635 to include a means to address multiple device receptacles. One of ordinary skill in the art would have been motivated to perform such a modification to utilize a multilevel security environment see '542 (col. 1, lines 14 et seq.) "This invention relates to computer security, and more particularly, to a multilevel computer security system and a method for controlling user access which allows a computer to be used in a multilevel security environment, but prevents access".

As to dependent claim 48, "in which the additional data-carrying object representing the principal comprises an image of the principal" is taught in '542 col. 6, lines 37-43 "The smart-card 30 has identification information about the card owner stored within its internal memory ... Biometrics are essentially a stored representation of a physical characteristic of the card owner".

As to dependent claim 49, "in which the additional data-carrying object representing the principal comprises a computer readable data portion and an image of the principal" is shown in in '542 col. 6, lines 37-43.

As to dependent claim 50, "further comprising a step of providing a holder for holding the computer- readable data portion such that both the computer- readable data portion and the image are accessible" is disclosed in in '542 col. 6, lines 37-43.

As to dependent claims 9, 23, 24, and 25 this claim incorporate substantially similar subject matter as in cited in the claims 33, 48, 49, and 50 above and are rejected along the same rationale.

12. **Claims 12, 17, 36, and 41** are rejected under 35 U.S.C. 103(a) as being unpatentable over '497 in further view of '635 in further view of Fehrman et al. U.S. Patent No. 6,193,163 (hereinafter '163).

As to dependent claim 36, "wherein the data-carrying objects is one of a pair of data-carrying objects" is taught in '635 col. 3, lines 63-67 "The security gateway generates a unique asynchronous key pair for each user and creates a token containing the private pair for each user and creates a token containing the private key for that particular user that is encrypted with the security gateway's";

the following is not taught in '497 and '635: **"and wherein the data-carrying objects in any given pair are fashioned so as to mechanically join together, and no two data-carrying objects not in the same pair will not or are unlikely to mechanically join together"** however '163 teaches "The first engagement member may comprise a first end portion of the

semiconductor chip assembly or a first tab extending from the semiconductor chip assembly" in col. 2, lines 44-59.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network security system taught in '497 and '635 to include a means to mechanically join two provided data key to protect devices. One of ordinary skill in the art would have been motivated to perform such a modification to protect data –carrying objects from tampering see '163 (col. 2, lines 4 et seq.) "Accordingly, there is a need for a smart card having an integrated circuit which may be removed or replaced by authorized personnel only. There is also a need for a smart card which provides an indication of tampering".

As to dependent claim 41, "wherein data objects in said group mechanically join together to form an assemblage, where the assemblage is adapted to be attached to a device through a single connection" is taught in '163 col. 6, lines 10-15 "Accordingly, it is an object of the present invention to provide a smart card having an integrated circuit which may be removed or replaced only by authorized personnel having a special tool".

As to dependent claims 12 and 17, these claims incorporate substantially similar subject matter as in cited in the claims 36 and 41 above and are rejected along the same rationale.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
23 July 2005

David Y. Jung
Primary Examiner
7/23/05